

REMARKS

Claims 1-10 and 12-14 are pending in this application. By this Amendment, claims 1 and 7 are amended to correct informalities Applicant discovered on review of the claims in preparation for filing this response. Claims 15-19 are canceled without prejudice to, or disclaimer of, the subject matter recited in those claims, as drawn to a non-elected invention. Reconsideration based on the above amendments and the following remarks is respectfully requested.

Entry of the amendments is proper under 37 C.F.R §1.116 since the amendments: (a) place the application in condition for allowance for the reasons discussed below; (b) do not raise any new issue requiring further search and/or consideration because the amendments simply correct obvious informalities and cancel claims drawn to a non-elected invention; and (c) place the application in better form for Appeal, should an Appeal be necessary. The amendments are necessary and were not earlier presented because they are made in response to the recent Restriction Requirement and to correct informalities as noted above. Entry of the amendments is thus respectfully requested.

Applicant appreciates the courtesies shown to Applicant's representative by Examiner LaForgia in the September 13, 2005 personal interview. Applicant's separate record of the substance of the interview is incorporated into the following remarks.

The Office Action, in paragraph 7, rejects claims 1, 2, 4, 5, 10 and 12 under 35 U.S.C. §103(a) as being unpatentable over U.S. Patent No. 6,330,677 to Madoukh in view of U.S. Patent No. 6,292,790 to Krahn et al. (hereinafter "Krahn"). The Office Action, in paragraph 18, rejects claim 3 under 35 U.S.C. §102(e) as being anticipated by Madoukh. The Office Action, in paragraph 20, rejects claims 6-9, 13 and 14 under 35 U.S.C. §103(a) as being unpatentable over Madoukh in view of Krahn and further in view of U.S. Patent

No. 6,173,400 to Perlman et al. (hereinafter "Perlman"). These rejections are respectfully traversed.

Madoukh teaches a system for authenticating processes and inter-process messaging with security performed in three layers -- an application layer, a middleware layer and a transport layer (Abstract). The security software disclosed in Madoukh directs a processor to (1) receive a request to authenticate a process, (2) authenticate the process, (3) generate a security association for the process, (4) store the security association, (5) transfer the security association, (6) receive the security association extracted from a message, and (7) check the security association extracted from the message with stored security association to authenticate the message (Abstract, emphasis added). The subject matter of Madoukh is not directed to an access privilege transferring method for safely transferring access privileges between clients, and between clients and servers, despite the assertion to the contrary in the Office Action.

First, Madoukh does not disclose applying a predetermined calculating operation to information comprising at least privilege information and search information, despite the Office Action's contrary assertions. The Office Action asserts that Madoukh teaches, among other features, applying a predetermined calculating operation to information comprising at least the privilege information and the secret information, thereby generating protected privilege information by the at least the first of the plurality of clients as is recited, among other features, in independent claim 1, and varyingly recited in independent claims 6 and 8. In support of this assertion, the Office Action cites the disclosure of Madoukh at col. 4, lines 42-63, and col. 5, lines 18-40. In these passages, Madoukh teaches a mathematical function that the Office Action appears to allege corresponds to a predetermined calculating operation.

The mathematical function in Madoukh, however, is applied to a system-generated random number in order to generate a result, that result being subsequently encrypted. The system then transfers the user ID, random number and encrypted result (*i.e.*, random number, subjected to a mathematical function, then encrypted) to a second system. The second system processes the random number with the same mathematical function to generate a result for comparison with a decrypted version of the transferred encrypted result (col. 4, line 55 - col. 5, line 6, and col. 5, lines 32-51). The mathematical function taught by Madoukh affects only the system-generated random number. As such, Madoukh cannot reasonably be read to teach the feature "applying a predetermined calculating operation to information comprising at least the privilege information and the secret information."

Second, the Office Action's assertion regarding Krahn is incorrect. Krahn teaches an apparatus to import and export computer configuration data, part of which is confidential, to and from plain-text computer files (col. 1, lines 17-19). As such, Krahn does not relate to an access privilege transferring method for safely transferring access privileges between clients, and between clients and servers, to which the subject matter of the pending claims is directed. Nor is Krahn directly related to a system that authenticates processes and inter-process messaging, such as that disclosed in Madoukh.

The Office Action concedes that Madoukh does not disclose applying a predetermined calculating operation to information comprising at least the privilege information and the secret information, thereby generating protected privilege information by the server. Rather, the Office Action relies on Krahn as disclosing such a feature. This reliance is misplaced. At, for example, paragraph 10, the Office Action states "Krahn teaches hashing a password and comparing it against stored hashed passwords." The Office Action then concludes that it would have been obvious to one of ordinary skill in the art at the time the invention was made to apply a predetermined calculation to the information (*i.e.*, one-way hash) and comparing

the protected information with the generated protected information, since Krahn states at col. 2, lines 9-12, that the server does not store plain-text passwords, thereby preventing unauthorized access from obtaining every user's password. This conclusion is incorrect, as explained below.

Krahn teaches that one common solution for protecting passwords when written to a text file is to hash them in a one-way hash (col. 2, lines 1-3). Krahn states further, in the Background of the Invention, that "[o]ne limitation of one-way hash schemes is that the original cleared-text password is not preserved on the server which is undesirable at the plain-text password is needed for another server purpose" (col. 2, lines 9-12, emphasis added).

Claim 1 recites, among other features, that the method comprises holding user information and secret information by each of a plurality of clients; holding, in a server, the user information and the secret information of at least a first of the plurality of clients. The method recited in claim 1 applies a predetermined calculating operation to information comprising at least the privilege information and the secret information by the at least the list of the plurality of clients, and separately applies the predetermined calculating operation to information comprising at least the privilege information and the secret information, thereby generating protected privilege information by the server for comparison. As such, the secret information (i.e., password information) is not destroyed but rather maintained. In the subject matter of the pending claims, it is the application of the predetermined calculating operation to the information for comparison that either provides or denies access to the objects. Therefore, Krahn cannot be considered to teach, or even to have suggested the feature applying a predetermined calculating operation to information comprising at least the privilege information and the secret information, thereby generating protected privilege information by the server, as is recited, among other features in independent claim 1, and varyingly recited in independent claims 3 and 4.

It should also be noted also that Krahn discloses this one-way hash as a disadvantage in the prior art systems that the invention in Krahn is intended to overcome. As such, the one-way hash of the password discussed in Krahn is not, in fact, the invention of Krahn.

Further, claims 2, 5, 7 and 9 are also not suggested by the combination of the applied references for at least their dependence on the above enumerated independent claims, as well as for the separately patentable subject matter that each of these claims recites.

Applicant's representative discussed the above arguments at least regarding the applicability of Madoukh and Krahn to the features of applying a predetermined calculating operation as recited in the claims, and the lack of any motivation to combine Madoukh and Krahn, with Examiner LaForgia during the September 13 personal interview. The Examiner did not rebut Applicant's arguments and indicated that he would further consider the arguments and take appropriate action upon filing of a formal response.

For at least these reasons, any conclusion that one of ordinary skill in the art would have been motivated to combine the teachings of Krahn with the teachings of Madoukh in order to find the subject matter recited in claims 1-9 to have been obvious is inaccurate and unsupportable. Additionally, there is nothing in Perlman which remedies the shortfalls in the application of Madoukh and Krahn to the subject matter recited in the pending claims.

Independent claim 10, and in like manner independent claims 12-14, recites steps of holding user information and secret by each of a plurality of clients; holding, in a server, the user information and the secret information of at least a first of the plurality of clients; generating privilege information by the at least the first of the plurality of clients; encrypting the generated privilege information by using the secret information, thereby generating protected privilege information by the at least the first of the plurality of clients; transmitting, from the at least the first of the plurality of clients; the user information and the protected privilege information to at least a second of the plurality of clients; retransmitting, by the at

least the second of the plurality of clients, the user information and the protected privilege information to the server, thereby making a request to access an object; decrypting the protected privilege information by using the secret information corresponding to the user information, thereby generating privilege information by the server; checking, by the server, whether the privilege information generated by the server is valid; and allowing access to an object in accordance with the result of the validity check.

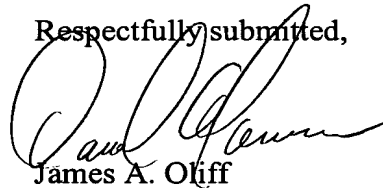
Many of these features are not specifically addressed in the rejections of these claims in the Office Action. As such, these rejections are improper. To the extent that a combination of Madoukh, Krahm, and Perlman may be applied to the recited features, Applicant respectfully submits that, for at least the reasons enumerated above, the references are not combinable. If Applicant's conclusion in this regard is incorrect, any permissible combination of the applied references would not have rendered obvious the combinations of features recited in claims 10 and 12-14.

Accordingly, reconsideration and withdrawal of the rejections of claims 1-10 and 12-14 under 35 U.S.C. §§102(e) and 103(a) as being anticipated by, or unpatentable over, Madoukh alone, or in combination with Krahm and/or Perlman, are respectfully requested.

In view of the foregoing, Applicant respectfully submits that this application is in condition for allowance. Favorable reconsideration and prompt allowance of claims 1-10 and 12-14 are respectfully requested.

Should the Examiner believe that anything further would be desirable in order to place this application in even better condition for allowance, the Examiner is invited to contact Applicant's undersigned representative at the telephone number set forth below.

Respectfully submitted,



James A. Oliff

Registration No. 27,075

Daniel A. Tanner, III

Registration No. 54,734

JAO:DAT/fpw

Date: September 19, 2005

OLIFF & BERRIDGE, PLC
P.O. Box 19928
Alexandria, Virginia 22320
Telephone: (703) 836-6400

**DEPOSIT ACCOUNT USE
AUTHORIZATION**

Please grant any extension
necessary for entry;
Charge any fee due to our
Deposit Account No. 15-0461